REMARKS

The Examiner has rejected Claims 1, 3-6, 8-11, 13-16, 18-22, and 25-27 under 35 U.S.C. 103(a) as being unpatentable over Drake et al. (U.S. Patent No. 6,347,374), in view of Porras et al. (U.S. Patent No. 6,704,874). Applicant respectfully disagrees with such rejection.

To establish a *prima facie* case of obviousness, three basic criteria must be met. First, there must be some suggestion or motivation, either in the references themselves or in the knowledge generally available to one of ordinary skill in the art, to modify the reference or to combine reference teachings. Second, there must be a reasonable expectation of success. Finally, the prior art reference (or references when combined) must teach or suggest all the claim limitations. The teaching or suggestion to make the claimed combination and the reasonable expectation of success must both be found in the prior art and not based on applicant's disclosure. *In re Vaeck,* 947 F.2d 488, 20 USPQ2d 1438 (Fed.Cir.1991).

Applicant respectfully asserts that at least the third element of the *prima facie* case of obviousness has not been met since the combination of Drake and Porras fail to teach all of applicant's claim limitations.

With respect to independent Claims 1, 6, 11, 16, and 21, the Examiner has admitted that Drake does not teach "a plurality of zone controllers coupled to the host controllers for analyzing an output of the host controllers," and "executing security actions in response thereto" (see same or substantially similar language in each of the above mentioned claims). Despite the prior art's failure to disclose the above claim language, the Examiner has rejected such language by stating that "[i]t is obvious at the time of the invention for one of ordinary skill in the art to separate both components to minimize the processing time and load."

PAGE 5/10 * RCVD AT 4/1/2005 4:13:55 PM [Eastern Standard Time] * SVR:USPTO-EFXRF-1/2 * DNIS:8729306 * CSID:408 971 4660 * DURATION (mm-ss):03-30

Applicant respectfully asserts that it would not have simply been obvious for one of ordinary skill in the art to separate both the host controllers and the zone controllers, as claimed by applicant. Specifically, Drake does not disclose any separate controller for "analyzing an output of the host controllers," and "executing security actions in response thereto." Applicant argues that separate zone controllers capable of analyzing and executing security actions, as claimed by applicant, provide for specific advantages not met by the prior art.

Not only do the separate zone controllers minimize processing time and load as the Examiner has suggested, but separate zone controllers also provide a complete solution of monitoring and detecting problems on a corporate enterprise level without requiring modules on every switch in the network since the zone controllers are each associated with a plurality of host controllers. In addition, this provides a solution that may fully scale to any size corporate network. Furthermore, the zone controllers are adapted to be associated with certain zones within a network. Applicant notes that the foregoing advantages are only some of the advantages of maintaining separate host and zone controllers, and that for these and other reasons such separation would not have been obvious to one of ordinary skill in the art.

With respect to all of the independent claims, the Examiner has admitted that Drake does not teach applicant's claimed "wherein a report is generated including a plurality of objects in a tree representation." The Examiner has stated that a "report in a tree representation is the designer choice." Applicant respectfully asserts that a report in a tree representation is not simply a designer choice since not all information is capable of being displayed in that way. For instance, Drake specifically teaches reports utilizing bar charts and reports in tabular format (see Col. 17, lines 25-59), but fails to disclose any report "including a plurality of objects in a tree representation," as claimed by

PAGE 6/10 * RCVD AT 4/1/2005 4:13:55 PM [Eastern Standard Time] * SVR:USPTO-EFXRF-1/2 * DNIS:8729306 * CSID:408 971 4660 * DURATION (mm-ss):03-30

applicant. Thus, Drake's invention does not support the creation of reports in a tree representation and therefore such would simply not be a designer choice.

Still yet, the Examiner has relied on Porras (col. 3 line 15 to Col. 4, line 67; Col. 7 line 18-Col. 8, line 67) to meet applicant's claimed "wherein a Simple Network Management Protocol (SNMP) trap capability is utilized." Applicant respectfully asserts that the only mentioning of SNMP in Porras is in relation to "networks being monitored...include[ing] features common to many network operating systems such as...SNMP..." (col. 3, lines 46-54) and "the monitors 22 may format their respective alert streams in a variety of formats, such as...SNMP..." (col. 4, lines 1-3). The Examiner has not only mistakenly relied on such excerpts since they relate to types of networks being monitored and to formats of alerts, but has also mistakenly relied on (Col. 7, line 18-Col. 8 line 67) which altogether fails to even mention SNMP, let alone an SNMP trap capability. Thus, "wherein a Simple Network Management Protocol (SNMP) trap capability is utilized," as claimed by applicant, is simply not met by the prior art.

With respect to independent Claim 22, the Examiner has relied on the same rejection as that given with respect to independent Claims 1, 6, 11, 16 and 21, along with Drake's disclosed "specifics of implementation...var[y] based on an audit source" (Col. 5, lines 36-60) and Drake's disclosed functionality of a "manager/configuration GUI" (Col. 17, lines 1-24). In relying on such excerpts from Drake, the Examiner has failed to address the claim language of Claim 22 not incorporated into the other above mentioned independent Claims, namely:

> "identifying a plurality of business rules;" and
> "providing services utilizing the information based on the business rules."

PAGE 7/10 * RCVD AT 4/1/2005 4:13:55 PM [Eastern Standard Time] * SVR:USPTO-EFXRF-1/2 * DNIS:8729306 * CSID:408 971 4660 * DURATION (mm-ss):03-30

Applicant respectfully asserts that Drake's teachings of audit analysis and of a manager/configuration GUI, as mentioned above, simply do not even suggest "business rules" in the manner claimed by applicant. Specifically, there is simply no mention in Drake of utilizing business rules in any way, and especially not to "provid[e] services utilizing the information based on business rules."

Again, applicant respectfully asserts that at least the third element of the *prima facie* case of obviousness has not been met, since the prior art references fail to teach or suggest all of the claim limitations. A notice of allowance or a specific prior art showing of the foregoing claimed features, in combination with the remaining claim elements, is respectfully requested.

Applicant has further noted that the prior art is deficient with respect to the dependent Claims. With respect to Claims 29 and 37, the Examiner has relied on Drake's disclosed "method of delivering the audit data to the next downstream process" wherein "audit data can be acquired and processed using either of the following modes: (a) batch mode; (b) real time mode" (Col. 8, line 43-Col. 9, line 15) to make a prior art showing of applicant's claimed "wherein enterprise latency mapping is performed" (Claim 29) and "wherein differences in delay times are calculated to construct a picture of latency throughout an enterprise" (Claim 37). Applicant respectfully asserts that a method of delivering audit data does not even relate to enterprise latency.

With respect to Claim 30, the Examiner has relied on the following excerpt from Porras to meet applicant's claimed "wherein at least on of the zone controllers chooses a port number associated with an application."

> "The alert manager can act as a sender or receiver. In embodiments, useful, for example, the alert manager can listen to a specified port in a network or connected to an external process on a host computer and process its data." (Col. 2, lines 12-17)

PAGE 8/10 * RCVD AT 4/1/2005 4:13:55 PM [Eastern Standard Time] * SVR:USPTO-EFXRF-1/2 * DNIS:8729306 * CSID:408 971 4660 * DURATION (mm-ss):03-30

Applicant respectfully points out that simply listening to a specified port, as disclosed in Porras, does not meet applicant's claimed "wherein at least one of the zone controllers chooses a port number associated with an application" because Porras fails to even mention choosing the specific port according to an application associated with the port, wherein a zone controller performs the choosing.

With respect to Claims 31 and 32, the Examiner has relied on Drake's disclosed "event detection system expert system engines fall into several categories...rule-based processors" and Drake's subsequent teaching of rule-based processing (Col. 11, line 7-Col. 12, line 10), along with Drake's disclosed "manager/configuration GUI" and "auditor/investigator GUI" (Col. 16, lines 53-57) to make a prior art showing of applicant's claimed "wherein the at least one zone controller pushes a configuration request to a plurality of the host controllers in an associated zone" (Claim 31) and "wherein the host controllers push the configuration request to the agents" (Claim 32). Drake's mere mention of a configuration GUI simply does not rise to the specificity of applicant's claim language, since applicant clearly claims a zone controller pushing "a configuration request to a plurality of the host controllers in an associated zone" and a "host controller push[ing] the configuration request to the agents" (emphasis added).

With respect to Claim 35, the Examiner has relied on Drake's disclosure of a "generalized database storage architecture" (Col. 5, lines 20-30) to make a prior art showing of applicant's claimed "wherein the monitor data is buffered." Simply stating that database storage is utilized does not inherently require data to be buffered, and furthermore, the entire Drake reference fails to make any suggestion of buffering monitored data.

With respect to Claim 36, the Examiner has relied on Drake's disclosure of " a set of graphical user interfaces" (Col. 16, lines 53-67; Fig. 1, item 16) to make a prior art showing of applicant's claimed "wherein the host controllers update the at least one

PAGE 9/10 * RCVD AT 4/1/2005 4:13:55 PM [Eastern Standard Time] * SVR:USPTO-EFXRF-1/2 * DNIS:8729306 * CSID:408 971 4660 * DURATION (mm-ss):03-30

Again, a notice of allowance or a specific prior art showing of the foregoing claimed features, in combination with the remaining claim elements, is respectfully requested.

In the event a telephone conversation would expedite the prosecution of this application, the Examiner may reach the undersigned at (408) 505-5100. Applicants are enclosing a check to pay for the added claims. The Commissioner is authorized to charge any additional fees or credit any overpayment to Deposit Account No. 50-1351 (Order No. NAIIP065_01.307.01).

Respectfully submitted,
Zilka-Kotab, PC

Kevin J. Zilka
Registration No. 41,429

P.O. Box 721120
San Jose, CA 95172-1120
408-505-5100

PAGE 10/10 * RCVD AT 4/1/2005 4:13:55 PM [Eastern Standard Time] * SVR:USPTO-EFXRF-1/2 * DNIS:8729306 * CSID:408 971 4660 * DURATION (mm-ss):03-30